NATIONAL PROGRAM OFFICE

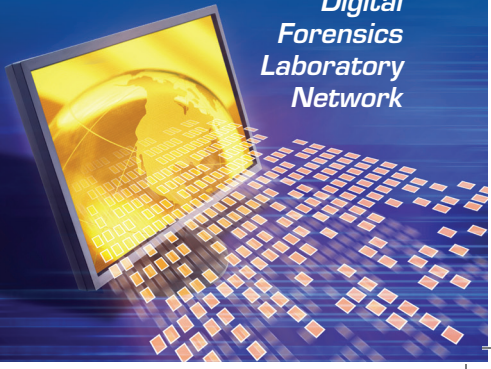
RCFL

CONTINUING EDUCATION SERIES

An Ongoing Training Initiative That Provides Law Enforcement and First Responders with the Latest Information They Must Know About Digital Evidence.

To access the Series online, visit www.rcfl.gov.

The RCFL Program—America's Premier Digital Forensics Laboratory Network



5 KEY FACTS ABOUT MOBILE FORENSICS

1. **Assess the Situation.** When handling mobile phones, there are good reasons for leaving the device on or powering it off. Assess the situation first before taking any action and determine what type of information you want.

2. **Don't Browse.** Scrolling through a suspect's mobile phone may alter evidence. If a phone is left at a crime scene, investigators may need to scroll through the phone to see the last person(s) called. In this situation, document what was previewed, and what, if any precautions were taken.

3. **Look for Peripherals.** When seizing mobile devices, look for "peripherals" such as cables, chargers, and SIM cards.

4. **Passwords Can Be Found.** If you encounter a SIM password, the service provider can help. But first, you'll need to obtain the proper search authority to enlist their assistance in obtaining this information.

5. **Don't Assume that Digital Evidence was Destroyed.** Mobile devices, including phones that have been in fires, submerged in water, encased in concrete, broken, bloody, or old, can still contain digital evidence. Seize the device and bring to a digital forensics Examiner for a full examination.

Request an archive version of the RCFL Program's "Managing Mobile Forensics: What Every Peace Officer Must Know" Webcast by logging onto

WWW.RCFL.GOV